

UNITED STATES DISTRICT COURT

March 18, 2019

for the
Southern District of Texas

David J. Bradley, Clerk of Court

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)5407 HARBOR LIGHT DRIVE
DICKINSON, TEXAS 77539

Case No. 3:19-mj-23

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A.

located in the Southern District of Texas, there is now concealed (identify the person or describe the property to be seized):
See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC 2252 and 2252A et seq.	Possession, Receipt and Distribution of Child Pornography

The application is based on these facts:

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

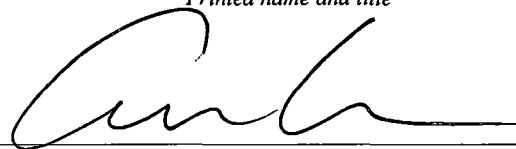

Applicant's signature

DeWayne Lewis, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 3-18-19


Judge's signature

City and state: Galveston, Texas

Andrew M. Edison, United States Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS

IN THE MATTER OF THE SEARCH OF
5407 HARBOR LIGHT DRIVE,
DICKINSON, TEXAS 77539

Case No. **G - 19 - 023**

**AFFIDAVIT IN SUPPORT OF AN APPLICATION
FOR A WARRANT TO SEARCH AND SEIZE**

I, DeWayne Lewis, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a warrant to search 5407 Harbor Light Drive, Dickinson, Texas 77539, hereafter referred to as the PREMISES, including its curtilage and associated vehicles. The residential PREMISES is more particularly described as a brown and beige brick, single-story house white trim. The home is on the east side of Harbor Light Drive and faces west. There are two white garage doors on the left (north) side of the house. The numbers 5407 are black on a white background affixed to the black mailbox at the edge of the street next to the concrete driveway. The residence is frequented by a white, 2012 Ford passenger car bearing Texas license plate KPZ0697, whose registration is listed at the PREMISES.

2. I am a Special Agent (SA) with the Department of Homeland Security, Immigration and Customs Enforcement (ICE), assigned to the Homeland Security Investigations (HSI) office in Galveston, Texas. I have been so employed since June 2002. As part of my duties as an ICE agent, I investigate criminal violations related to child exploitation and child pornography, including violations pertaining to online extortion and/or stalking, adults attempting to meet with juveniles for sexual encounters and the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 875(d), 2422(b), 2423, 2251, 2252, 2252A and 2261A(2). I have received training in the area of child pornography and

child exploitation, and I have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256)¹ in all forms of media, including computer media. I have participated in the execution of numerous search warrants and covert operations involving child exploitation and the online solicitation of minors, many of which involved child exploitation and/or child pornography offenses. I am in routine contact with experts in the field of computers, computer forensics, and Internet investigations. I annually attend the Dallas Crimes Against Children Conference where I attend various investigative training. I am currently a member of the Houston Metro Internet Crimes Against Children Task Force. This task force includes prosecutors and members of multiple police agencies across the southeast/coastal Texas and Houston metro regions.

3. This investigation initially involved a suspect who was posting and/or saving nude images of minor children in his Dropbox virtual storage account. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. As a result of the investigation described more fully below, there is probable cause to believe that evidence of a crime, contraband, fruits of a crime, and other items illegally possessed in violation of federal law, including 18 U.S.C. §§ 2252 and/or 2252A, et seq. are

¹ “Child Pornography means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where – (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; . . . [or] (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.” For conduct occurring after April 30, 2003, the definition also includes “(B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from that of a minor engaging in sexually explicit conduct,” 18 U.S.C. § 2256(8).

present at the PREMISES and/or within the custody and control of the person using email address rick5408@hotmail.com and Dropbox Screen/User name “John Smith.”

TECHNICAL TERMS

5. **Internet:** The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

6. **IP Address:** The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). This design is known in the industry as “IPV4” version of internet protocol addresses. Every computer, and/or device attached to the Internet, must be assigned an IP address so that Internet traffic sent from, and directed to, that computer may be directed properly from its source to its destination. When the internet was in its infancy there was an assumption that IPV4 would be sufficient to service the world's future IP Address needs. Over time it became clear this assumption was wrong and that the 4.3 billion IP addresses created with IPv4 would soon run out. The last remaining IPv4 Internet addresses were allocated by ICANN (the Global custodian and governing body of the Internet) in February 2011. The solution was to create a new version with many more addresses, which is what the internet industry has done with Version 6 (IPv6). The IPV6 versions of IP addresses resemble this one: 2602:30a:c00c:1c19:39be:c529:89aa:859. This transition, which has already begun, may take up to a decade or longer. The new version will create an almost limitless supply of IP addresses, in anticipation that nearly all technology in the future will be connected via the internet. Version 6 will have 3.4 billion-to-the-fourth power IP addresses

available for allocation. That is enough IP addresses for every single device utilizing this Protocol, virtually into perpetuity. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

7. **Dropbox:** Dropbox is a service that allows its users to store files on Dropbox's servers. According to the Dropbox privacy policy, Dropbox collects and stores files that are uploaded, downloaded, or accessed with the Dropbox service. Dropbox also collects logs, which includes information from the customer's device, its software, and customer activity using the Dropbox services. That information can include the customer's device's Internet Protocol ("IP") address, browser type, the web page the customer visited before he went to the Dropbox website, information searched for on the DropBox website, locale preferences, identification numbers associated with the customer's devices, their mobile carrier, date and time stamps associated with transactions, system configuration information, metadata concerning a customer's files, and other interactions with the Drobox services. Dropbox is a free service that allows customers to bring all their files, photos, documents, and videos anywhere. That means that any file a customer saves to their Dropbox account will automatically be accessible via all of the customer's computers, phones and even the Dropbox website.

8. **Apple, Touch ID and Face ID:** I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices, such as iPhones and iPads, offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") in lieu of a numeric, or alphanumeric, passcode or password. This feature is called Touch ID. More

recently, iPhones and iPads offer the same unlock feature via facial recognition referred to as Face ID.

9. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center on the front of the device. In my training and experience, users of Apple devices that offer Touch ID and Face ID often enable it because it is considered to be a more convenient way to unlock the device than by entering the passcode, as well as a more secure way to protect the device's contents. This is particularly true when the user of the device is engaged in criminal activities and thus has a heightened concern about securing the contents of the device.

10. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) five unsuccessful attempts to unlock the device via Touch ID are made.

11. In my training and experience, the person who is in possession of a device, or has the device among his or her belongings at the time the device is found, is likely a user of the device. However, in my training and experience, that person may not be the only user of the

device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the PREMISES to press their finger(s) against the Touch ID sensor of the locked Apple device(s) found during the search of the PREMISES in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID, or, if their Apple device is a more recent iteration, Face ID.

PROBABLE CAUSE

12. The Houston Metro Internet Crimes Against Children (ICAC) task force received information about suspicious activity from a cloud service company named Dropbox, Inc. Dropbox reported to the National Center for Missing and Exploited Children (NCMEC) on December 10, 2018, that someone was using their cloud services to store or transfer suspicious images of nude minors via the internet. Dropbox viewed 27 files that were publicly available and provided those images to NCMEC. The report was forwarded to the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (HSI) office in Galveston, Texas. HSI Special Agent DeWayne Lewis received and reviewed the report. There were 27 suspicious files that consisted of images and videos depicting nude minor children exposing their genitals and/or engaging in sexual activity. The Dropbox customer information associated with the account was, in part:

Email Address: rick5408@hotmail.com

Screen/User Name: John Smith

IP Address: 2601:2c4:c680:677:40cc:dae8:d733:297c (Login) 09-26-2018 15:21:46 UTC

The IP address, 2601:2c4:c680:677:40cc:dae8:d733:297c, was one managed by the internet service provider Comcast.

13. Houston Police Department Officer Wendy Corrales, who is also a member of the Houston Metro ICAC, had a subpoena issued to Comcast on October 16, 2018 to identify the service address for the customer assigned IP address 2601:2c4:c680:677:40cc:dae8:d733:297c at the time and date listed in paragraph 12 above. Comcast responded on October 17, 2018 with the following information, in part:

Service Address:	5407 HARBOR LIGHT DR DICKINSON, TX 77539-6522
Telephone #:	281-337-4377
Type of Service:	High Speed Internet Service
Account Number:	8777701110364459
Account Status:	Active
IP Assignment:	Dynamically Assigned

14. Special Agent Lewis examined the suspicious files that Dropbox viewed and reported to NCMEC from “John Smith’s” Dropbox activity. The following examples fit the federal definition of child pornography and are from that collection of files:

partial title: 8c0474f3...mp4: was a color video that depicted a topless Caucasian minor female, approximately 4-7 years old, lying on her back while an adult Caucasian male wearing light blue shorts inserted his erect penis into the minor’s mouth, continued masturbating and ejaculated into the girl’s mouth and on her chest for the camera’s view.

title: 000001420 2 (1).wmv: was a color video that depicted a nude Caucasian minor female, approximately 6-8 year old, lying prone on her back while an adult Caucasian male wearing a light blue shirt inserted his erect penis into the minor’s anus for the camera’s view.

15. Special Agent Lewis had a federal search warrant served on Dropbox on February 5, 2019, for documentation and content. Dropbox responded with the requested information on February 13, 2019. SA Lewis reviewed the subscriber information, file activity logs and file contents. The subscriber information included the following, in part:

Name: John Smith
Email: rick5408@hotmail.com
User ID: 656585863
Joined: Mon, 20 Mar 2017 13:04:03 GMT
Subscription Status: Free

16. Special Agent Lewis reviewed the folder titles and the files contained within them. Some of the folder titles included, in part:

11 year old boy	young
12 year old girl	young boys
13 year old girl	young girls
14 year old boy	young girls 2
guys 12 year old sister	young pics
Under 10 – 12	young videos
kids	

Special Agent Lewis reviewed the image and videos files that consisted mostly of minor children displaying their genitals or performing sexual acts alone, with other children or with adults. Three of those examples that fit the federal definition of child pornography are listed below, in part:

title: Video Jun 19, 6 32 59 AM.mp4 was a color video in a bedroom setting that depicted a Caucasian minor female approximately 10-11 years old wearing black socks next to a nude Caucasian adult male lying in front of the minor on the bed while he masturbated. The video continued as the adult male pressed his erect penis against the minor's mouth as he ejaculated.

title: File May 08, 2 06 19 PM.jpg was a color image in a bathtub setting that depicted a nude Caucasian infant approximately 4-8 months old being supported in the water by adult Caucasian arms while her legs were spread to expose her vagina for the camera's view.

title: Photo Aug 22, 8 54 31.jpg was a color photo that depicted a Caucasian infant approximately 8-12 months old wearing only an orange shirt while an adult Caucasian hand held her right leg apart to expose her vagina for the camera's view.

17. Special Agent Lewis conducted surveillance on multiple different days in February of 2019, and observed a white Ford passenger car bearing Texas license plate DPZ0697. The registration for that car returned to the PREMISES. There also appeared to be another, smaller white car parked on the left side of the garage during one of SA Lewis' drive-bys, which was usually concealed by the closed garage door.

Characteristics Common to Individuals with a Sexual Interest in Children

19. Based upon my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the sexual exploitation of children which includes the distribution, receipt, possession and collection of child pornography:

- a. Individuals with a sexual interest in children receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.
- b. Individuals with a sexual interest in children collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals with a sexual interest in children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower, or "groom," the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to

demonstrate the desired sexual acts.

- c. Individuals with a sexual interest in children almost always possess and maintain their “hard copies” of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home, email account or in “virtual” storage, like in the iCloud or Dropbox.com. Individuals with a sexual interest in children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
 - i) “Child erotica,” as used in this Affidavit, is defined as materials or items that are sexually arousing to certain individuals, but which are not in and of themselves obscene or do not necessarily depict minors in sexually explicit poses or positions. Such material may include non-sexually explicit photographs (such as minors depicted in undergarments in department store catalogs or advertising circulars), drawings, or sketches, written descriptions/stories, or journals.
- d. Likewise, Individuals with a sexual interest in children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area or “virtual” storage. These collections are often maintained for several years and are kept close by, or remotely accessible, usually at, or via, the collector’s residence, to enable the collector to view his collection, which is highly valued.
- e. Individuals with a sexual interest in children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone

numbers of individuals with whom they have been in contact and who share the same interests in sex with children or child pornography.

- f. Individuals with a sexual interest in children prefer not to be without their child pornography, or prohibited from its' access, for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

20. Based upon my training, knowledge and experience in investigations related to child exploitation and my conversations with other law enforcement officers who have engaged in numerous investigations involving child pornography and exploitation, I am aware that individuals who access paid subscription or free sites offering images and/or videos depicting child pornography do so for the purpose of downloading or saving these images to their hard drive or other storage media so that the images and videos can be added to their collection. I know that individuals involved in the distribution of child pornography also continue to obtain images of child pornography found elsewhere on the Internet such as newsgroups and websites, and via paid subscriptions, as well as their own "trophy photos" of sexual conquests involving the exploitation of children. Those trophy photos usually consist of photos they've produced of a live victim they've touched or a screen capture of a victim they've exploited online.

21. Additionally, based upon my training, knowledge and experience in investigations related to child exploitation and child pornography cases, I am aware that individuals who have a sexual interest in children will oftentimes have a collection of child pornography and will ask children to take and send naked images of the themselves that would constitute child pornography as well as child erotica.

22. Furthermore, based upon my training, knowledge and experience in investigations

related to child exploitation and child pornography cases, I am aware that individuals who have a sexual interest in children will oftentimes utilize social media such as Snapchat, Instagram, Kik Messenger, Twitter, Facebook, WhatsApp, ChatStep, Skout, Grindr, Craigslist and other online services to meet and communicate with minors. Individuals with a sexual interest in children know that social media allows for seemingly anonymous communication which they can then use to groom the minors and set up meetings, whether in person or online, in order to sexually exploit them.

Computers and Child Pornography

23. Based upon my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers and computer technology (including advances in smartphones, tablets and internet connectivity) have revolutionized the way in which children are exploited and how child pornography is produced, distributed, and utilized. Advancements in cellular telephone technology and mobile applications have furthered those revolutionary methods of exploitation.

24. Cellular telephones are routinely connected to computers to re-charge the batteries and synchronize the mobile telephone with their matching computer programs, or “applications,” on the computer. Cellular telephones are connected to the user’s computer to transfer, save or back-up files or to download files, programs or “applications” via the internet, as one would do for music or ring tones. Users connect their cellular telephones to their computer to save, or back-up, their content or upload those files via the internet to a virtual storage medium like the iCloud or Dropbox, which allow users to access that content from any device with internet access, including their mobile devices (cellular phones or tablets) or another computer. Users can also download programs to their computers that mimic, or operate as if they are using,

applications on their cellular telephone. Some of those examples include “iPadian,” “Andy,” and “BlueStacks.” People with a sexual interest in children have embraced these technologies in their efforts to exploit children, conceal their true identities, misdirect investigators, hide evidence and communicate with others with the same interests.

25. Technologies for portable cellular telephones, their batteries, internet connectivity and quick-charge devices have also greatly advanced. Today’s vehicles often advertise built-in options for internet connectivity. In early 2013, General Motors announced it would partner with AT&T to outfit most of its 2014 models with high-speed data connectivity, with those same options available from Chrysler, Audi and Ford. These portable devices are commonly stored and used in vehicles and derive their power from being plugged in to cigarette lighters or auxiliary power outlets. Other portable navigation devices, like the Garmin or TomTom, provide turn-by-turn directions to previously unknown locations when the user inputs the desired address or destination and are commonly kept or stored in the user’s vehicle. Many modern vehicles are equipped with satellite navigation from the factory. Modern computer technology in today’s vehicles can navigate you to your destination, synchronize your cellular telephone to the on-board monitor for hands-free use and adjust radio and environmental controls by responding to voice-activated commands. The suspects’ vehicles have increasingly become mobile storage places for evidence like the satellite navigation devices, laptops or storage media concealed from other household members. They also can hold other evidence linked to their travel for contact with like-minded adults and sexually exploited minors; like gasoline, toll booth and parking receipts or traffic tickets.

26. Prior to the advent of computers and the internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop

and reproduce the images. As a result, there were definable costs involved with the production of images. To distribute these images on any scale also required significant resources. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently, through the use of computer technology and the Internet, producers, collectors and distributors of child pornography can instantly and remotely upload images into virtual storage, like in the iCloud or Dropbox, allowing them to operate almost anonymously.

27. In addition, based upon my own knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, the development of computers (including cellular telephones) and wi-fi technology has also revolutionized the way in which those who seek child pornography are able to obtain this information. Computers, and the modern "smartphone," allow simplified, often anonymous communication with persons far-removed from the solicitor. They can communicate with others with similar interests or where laws against sex with children are more lax or less enforced. They can also communicate directly with minor victims in a safe environment believing that their communications are anonymous. Computers also serve four basic functions in connection with child pornography: production, communication, distribution, and storage. More specifically, the development and advancement of computers and internet technology has changed the methods used by those who seek to sexually exploit children and obtain access to child pornography in these ways.

28. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera, including cameras contained in the latest smartphones. A digital camera can be attached, using a device such as a cable, or digital images are often uploaded from the camera's memory card, directly to the computer. Images can then be

stored, manipulated, transferred, or printed directly from the computer. Images can be edited in ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. Because of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.

29. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers are sometimes operated by commercial ISPs, such as Comcast, AT&T and America Online (“AOL”), which allow subscribers to dial a local number or otherwise directly connect to a network, which is, in turn, connected to the host systems. Host computers, including ISPs, allow e-mail service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web.

30. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in sex with children or child pornography; and (ii) websites that offer images of child pornography. Those who seek to obtain images or videos of child pornography can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute or receive child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the

distributor and recipient, are well known and are the foundation of transactions involving those who wish to gain access to child pornography over the Internet. Sometimes, the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the recipient's computer, including the Internet history and cache² to look for "footprints" or "relics" of the websites and images accessed by the recipient.

31. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single compact disk can store thousands of images and pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 500 gigabytes and larger are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime." Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

32. Computer files, or remnants of such files, can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new

² "Cache" refers to text, image, and graphic files sent to and temporarily stored by a user's computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website.

data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is - in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

CONCLUSION

33. Based upon my own knowledge, experience and training related to child pornography and child exploitation investigations, I am aware that individuals who have a sexual interest in children who possess and/or distribute child pornography are often child pornography collectors. They often collect, or hoard, their images for the purposes of trading with others as a method of adding to their own vast collections. Furthermore, I know that individuals with a sexual interest in children and who are involved in the collection and distribution of child pornography also continue to obtain images of child pornography found elsewhere on the Internet, such as in newsgroups and other websites, including via paid-subscription sites. Sometimes those “payments” are in the form of new, or bartered, images depicting the sexual exploitation of a child.

34. Finally, based upon the conduct of individuals who have a sexual interest in children, who possess and collect child pornography, and who hoard, receive and distribute child

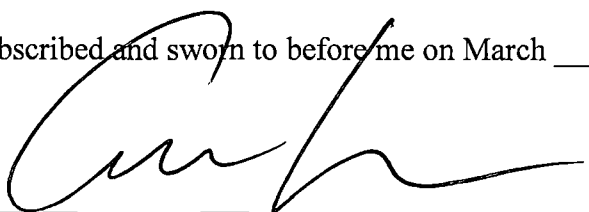
pornography, namely, that they tend to maintain their collections for long periods of time, even over the course of years, there is probable cause to believe that evidence of the offenses of Receipt, Distribution and Possession of Child Pornography is currently located at the PREMISES. I believe the suspect has demonstrated these offender characteristics based on his use of the internet to manipulate child exploitation material and his posting of multiple child pornography images onto his virtual storage account to view, save or share.

35. Based on the above information, there is probable cause to believe that evidence of violations of Title 18 U.S.C. §§ 2252 and 2252A, which, among other things, makes it a federal crime for any person to possess, receive or distribute child pornography, have been violated, and that any such property is evidence of a crime, fruits of a crime, contraband and other items illegally possessed and is located at the PREMISES occupied, maintained, and/or controlled by Marcus Howell.

Respectfully submitted,


DeWayne Lewis
Special Agent
DHS/ICE/Homeland Security Investigations

Subscribed and sworn to before me on March 18th, 2019


The Honorable Andrew M. Edison
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The premises to be searched is at 5407 Harbor Light Drive, Dickinson, Texas 77539, further described as a one story, brown and beige mottled brick house with white trim. It is on the east side of Harbor Light Drive facing west. The concrete driveway is on the left, which leads to the two, white garage doors. The numbers 5407 are in black on a white background and attached to the black mailbox on the street at the end of the driveway.

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. §§ 2251, 2252 and 2252A, those violations involving a suspect using email address rick5408@hotmail.com and Dropbox Screen/User name “John Smith,” including:
 - a. Records and information relating to Dropbox, multiple Dropbox accounts, other virtual storage accounts, email account rick5408@hotmail.com and/or any other email accounts, and alias named and or other “imposter” accounts;
 - b. Records and information relating to the identity or location of the suspect(s);
 - c. Records and information relating to communications with Internet Protocol address 2601:2c4:c680:677:40cc:dae8:d733:297c and any others utilized to track or log in to the various accounts;
 - d. Records and information relating to wiping, deleting or evidence-destroying software;
 - e. Records and information relating to the online solicitation of minors and the possession, receipt, distribution or production of child pornography.
2. Computers or storage media used as a means to commit the violations described above, including desktop computers, laptop computers, smartphones, tablets, hard drives, thumb drives, compact discs, storage discs, memory sticks or any other items with electronic or digital storage capacity.
3. For any computer, smartphone or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
 - e. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
 - f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - h. evidence of the times the COMPUTER was used;
 - i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
 - j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - k. records of or information about Internet Protocol addresses used by the COMPUTER;
 - l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
 - m. contextual information necessary to understand the evidence described in this attachment.
 - n. Any and all cameras, film, videotapes or other photographic equipment (including, but not limited to clothing, costumes and/or props).
4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include sim cards, hard disks, RAM, floppy disks, flash memory or "thumb drives," CD/DVD-ROMs, and other magnetic or optical media.